ENHANCED FORENSIC PROCESS MODEL IN CLOUD ENVIRONMENT

AHMED NOUR MOUSSA

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy (Computer Science)

School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia

DECEMBER 2018

Dedicated to my mother, Aisha Mouhoummed a strong and gentle soul who taught me to trust in God, and believe in hard work, and my sisters, Fathia, Fardousa and Nasra who without their supports, and most of all love, the completion of this work would not have been possible.

ACKNOWLEDGEMENT

First and foremost, I have to thank Allah for his blessings. Special words of thanks go to my supervisor, Assoc. Prof. Dr. Norafida Ithnin for her support, guidance, dedication, commitment, encouraging, belief in my abilities, consulting critical-thinking in me and profound interest in my research.

Special words of thanks also go to my wife, Amina Souleiman and my two sons Souleiman and Sultan and my daughter Hibah for their support, love, patience, understanding and tolerance in the entire duration of my studies.

I am grateful to the Ministry of Higher Education Malaysia for providing me financial support during the period of this research work.

ABSTRACT

Digital forensics practitioners have used conventional digital forensics process models to investigate cloud security incidents. Presently, there is a lack of an agreed-upon or a standard process model in cloud forensics. Besides, literature has shown that there is an explicit need for consumers to collect evidence for due-diligence or legal reasons. Furthermore, a consumer oriented cloud forensics process model is yet to be found in the literature. This has created a lack of consumer preparedness for cloud incident investigations and dependency on providers for evidence collection. This research addressed these limitations by developing a cloud forensic process model. A design science research methodology was employed to develop the model. A set of requirements believed to be solutions for the challenges reported in three survey papers were applied in this research. These requirements were mapped to existing cloud forensic process models to further explicate the weaknesses. A set of process models suitable for the extraction of necessary processes was selected based on the requirements, and these selected models constituted the cloud forensic process model. The processes were consolidated and the model was proposed to alleviate dependency on the provider problem. In this model, three digital forensic types including forensic readiness, live forensics and postmortem forensic investigations were considered. Besides, a Cloud-Forensic-as-a-Service model that produces evidence trusted by both consumers and providers through a conflict resolution protocol was also designed. To evaluate the utility and usability of the model, a plausible case scenario was investigated. For validation purposes, the cloud forensic process model together with its implementation in the case scenario and set of requirements were presented to a group of experts for evaluation. Effectiveness of the requirements was rated positive by the experts. The findings of the research indicated that the model can be used for cloud investigation and is rated easy to be used and adopted by consumers.

ABSTRAK

Pengamal forensik digital telah menggunakan model proses forensik digital konvensional untuk mengkaji isu-isu keselamatan awan. Pada masa ini, terdapat kekurangan dalam model proses yang standard atau dipersetujui dalam forensik awan. Selain itu, tinjauan literatur menunjukkan terdapat keperluan yang jelas untuk pengguna mengumpul bukti bagi ketelitian atau alasan undang-undang. Tambahan pula, kajian model proses forensik awan yang berorientasikan pengguna masih belum ditemui dalam kajian literatur. Ini telah mewujudkan kekurangan kesediaan pengguna untuk mengkaji isu-isu awan dan pergantungan pada pembekal untuk pengumpulan bukti. Kajian ini membincangkan batasan-batasan ini dengan membangunkan model proses forensik awan. Kaedah penyelidikan reka bentuk sains telah digunakan untuk membangunkan model. Satu set keperluan yang dipercayai menjadi penyelesaian bagi cabaran yang dilaporkan dalam tiga kertas kerja kajian telah digunakan dalam kajian ini. Keperluan ini telah dipetakan kepada model proses forensik awan yang sedia ada untuk menerangkan kelemahan dalam model. Satu set model proses yang sesuai bagi pengekstrakan proses yang diperlukan telah dipilih berdasarkan keperluan dan model terpilih ini membentuk model proses forensik awan. Proses itu disatukan dan model dicadangkan untuk mengurangkan kebergantungan kepada masalah pembekal. Dalam model ini, tiga jenis forensik digital termasuk kesediaan forensik, forensik hidup dan siasatan forensik postmortem dipertimbangkan. Di samping itu, model Forensik-Awan-sebagai-Perkhidmatan yang menghasilkan bukti yang dipercayai oleh pengguna dan pembekal melalui protokol resolusi konflik juga direka bentuk. Untuk menilai utiliti dan kebolehgunaan model, satu senario kes yang munasabah telah dikaji. Untuk tujuan pengesahan, model proses forensik awan bersama-sama dengan pelaksanaannya dalam senario kes dan set keperluan telah dibentangkan kepada kumpulan pakar untuk penilaian. Keberkesanan keperluan dinilai positif oleh pakar. Dapatan kajian menunjukkan bahawa model boleh digunakan untuk siasatan awan dan dinilai mudah digunakan dan diterima pakai oleh pengguna.

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGEMENT	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vii
	LIST OF TABLES	xii
	LIST OF FIGURES	xiv
	LIST OF APPENDICES	xvi
1	**INTRODUCTION**	**1**
	1.1 Overview	1
	1.2 Problem Background	2
	1.3 Problem Statement	6
	1.4 Research Questions	7
	1.6 Research Objectives	8
	1.6 Scopes of the Research	9
	1.7 Significance of The Research	10
	1.8 Organization of the Report	11
2	**LITERATURE REVIEW**	**13**
	2.1 Overview	13
	2.2 Cloud Computing	14

2.2.1 Cloud Computing Architecture 17

2.2.2 Role and Responsibilities in cloud Computing 20

2.3 Cloud Security Concerns 21

2.4 Digital Forensics 24

2.4.1 International Standards and Guidelines in Digital Forensics 26

2.5 Digital Evidence 27

2.6 Cloud Forensics 27

2.6.1 Cloud Forensics Challenges 30

2.6.2 Cloud Forensics process model requirements 33

2.6.3 Current Researches Focusing on Cloud Forensic Investigations 38

2.7 Applying Proposed Requirements against Existing Cloud Forensics Models 49

2.8 Digital Forensic Process Models Reviewed 53

2.9 Modeling Approaches for Digital Forensics Activities 72

2.10 Business Process Modelling and Notation (BPMN) 77

2.10.1 Process Modelling Guidelines 78

2.10.2 Model Transformation 80

2.11 Summary 82

3 RESEARCH METHODOLOGY 83

3.1 Overview 83

3.2 Selecting Design Science Research as a Research Paradigm 84

3.3 Design Science Research Model 85

3.4 Research Framework 87

3.4.1 Phase 1: Requirements definition and Problem Explication 90

3.4.2 Phase 2: Design and Develop 92

3.4.3 Phase 3: Demonstration 94

3.4.4 Phase 4: Evaluation 98

3.4.5 Phase 5: Cloud Forensic as a Service Model 101

3.5 Summary 101

4 **DESIGN AND DEVELOPMENT OF THE CLOUD FORENSIC PROCESS MODEL** **103**

4.1 Overview 103

4.2 Model Development Process 104

4.2.1 Identifying a Set of Source Models 104

4.2.2 Extraction of Processes in the models identified in step1 108

4.2.3 Short-listing Candidate Processes 114

4.2.4 Designating Processes into Three Digital Investigation Types 118

4.2.5 Determining the Relationship between Processes 130

4.2.6 Validating the Process Model 130

4.2.7 Result of the Validation Technique: Second Version of CFPM 146

4.3 Summary 153

5 **DEMONSTRATING AND EVALUATING THE MODEL** **154**

5.1 Overview 154

5.2 Scenario 1 156

5.2.1 Forensic Readiness Component 157

5.3 Scenario 2 163

5.3.1 Incident Detection and Preparation 164

5.4 Discussions of the Case Scenarios 174

5.4.1 Case Scenario 1 175

5.4.2 Case Scenario 2 176

5.5 Evaluating the Model 177

5.5.1 Identifying and Nominating Participants of the Evaluation 178

5.5.2 Feedback from the Participants 179

5.5.3 Evaluating the Requirements 180

5.5.4 Evaluating the Process Model 180

5.5.5 Details Feedback from the Evaluators 181

5.5.6 Discussions of the Evaluation 186

5.6 Evaluating CFPM Model Against the Requirements 190

5.7 Summary 194

6 TRUSTED CLOUD FORENSICS AS A SERVICE ON THE LIVE FORENSIC COMPONENT 195

6.1 Overview 195

6.2 Cloud Forensics as a Service 196

6.3 Root of Trust and Trust Assumptions 198

6.4 Bilateral CFaaS System 199

6.5 Forensic Data Collection 200

6.6 Agreement on Mutually Trusted Forensics Output 202

6.7 On the Feasibility of Bilateral Cloud Forensic as a Service (Validation) 206

6.8 Summary 210

7 CONCLUSION AND RECOMMENDATION 211

7.1 Overview 211

7.2 Summary of Research Problem Addressed 212

7.3 Research Contributions 214

7.4 Limitations of the Research 215

7.5 Future Research 217

REFERENCES 219

LIST OF TABLES

TABLE NO.	TITLE	PAGE
2.1	A Comparison of Cloud Delivery Model Control Levels	16
2.2	Cloud Consumers against Cloud Providers Activities	16
2.3	Cloud Forensic Process Model Requirements	37
2.4	Summary of Evaluated Cloud Forensic Process Models	51
2.5	Defining Investigative Objectives	62
2.6	Summary of the Reviewed Process Models	71
2.7	Seven Process Modeling Guidelines	79
3.1	Six Activities of DSRM and their Descriptions	87
4.1	Summary of the Assessment of the Inclusion Criteria	106
4.2	Selected Process Models	107
4.3	Source Models	108
4.4	Summary of the Processes and Sub-Processes in the Selected Process Models	110
4.5	Recurrence Process and their Similar Process in other Models	116
4.6	Reduced Processes and Sub-process Listing	117
4.7	Initial Designation of Processes	118
4.8	Readiness Processes and Sub-processes	123
4.9	Live Processes and Sub-processes	124
4.10	Postmortem Processes and Sub-processes	124
4.11	Cloud Forensics Process Models	132
4.12	Forensic Readiness Processes	133
4.13	Live Forensic Processes	134
4.14	Postmortem Forensic Processes	135
4.15	Continuous Processes	136
4.16	M01 against CFPM	136

4.17	M02 against CFPM	137
4.18	M03 against CFPM	138
4.19	M04 against CFPM	139
4.20	M05 against CFPM	140
4.21	M06 against CFPM	140
4.22	M07 against CFPM	141
4.23	M08 against CFPM	142
4.24	M09 against CFPM	142
4.25	M10 against CFPM	143
4.26	M11 against CFPM	145
4.27	M12 against CFPM	145
4.28	M13 against CFPM	146
4.29	Identified New Processes	147
5.1	SIEM Evaluation	159
5.2	Potential Log Sources within XYZ Corps Infrastructure	161
5.3	Identified IP Address	171
7.1	Criteria for Evaluating the Process Model	178
7.2	Model Requirement Achieved	193

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
2.1	Characteristics of Cloud Computing	15
2.2	Cloud Reference Architecture	17
2.3	Sample Components of IaaS Infrastructure	19
2.4	Contractual Relation Between the Two Parties	21
2.5	Mostly Cited Cloud Security Issues	22
2.6	Threats to Different Domains in Cloud	23
2.7	Security Requirements per Cloud Service Delivery Model and Deployment Models	23
2.8	Digital Forensic Use Case	68
2.9	EEDI Stages after Stephenson	72
2.10	Kruse & Heiser Activity Diagram	73
2.11	Kruse & Heiser Use Case Diagram	74
2.12	US Doj Activity Diagram	74
2.13	US DoJ Use Case Diagram	74
2.14	Forensic Process Use Case after Ruan and Huebner	75
2.15	Forensic Process Activity Diagram after Ruan	75
2.16	The Perambulation Procedure after Wang	76
2.17	MOF Framework, Horizontal and Vertical Transformation	81
3.1	Design Science Research Method (DSRM)	86
3.2	High Level View of the Research Methodology	88
3.3	Research Framework	89
3.4	Phase 1 Activities	92

3.5 Phase 2 Activities 93

3.6 Infrastructure in a VirtualBox 96

3.7 Phase 3 Activities 97

3.8 Phase 4 Activities 99

3.9 Phase 5 Activities 101

4.1 Readiness Component 125

4.2 Live Forensic Component 126

4.3 Postmortem Component 127

4.4 Validated Incident Detection and Preparation 150

4.5 Validated Live Investigation Component 151

4.6 Validated Postmortem Investigation Component 151

4.7 High-level Cloud Forensic Process Model 152

5.1 Uploaded Filename 169

5.2 Access Log Showing OwnCloud Server Access by the Suspect 172

5.3 Amended Postmortem Investigation Component 189

6.1 Cloud Forensic as a Service Components 197

6.2 Provider and Consumer of a Cloud Storage Forensics Services. 201

6.3 Model of Bilateral Data Collection 202

6.4 High Level View of the Bilateral Cloud Forensic as a Service 204

6.5 Bilateral Cloud Forensic as a Service Model. 205

6.6 Non-repudiable Sharing of Forensic Data 209

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	Conventional Digital Forensic Process Models	236
B	Processes Contained in the Selected Processes Models	245
C	Model Evaluation Form	252

CHAPTER 1

INTRODUCTION

1.1 Overview

Cloud forensics is important in investigating security incidents happening in cloud environments. However, some national and international standard organizations are currently busy working on the production of standard procedures that can be used by the cloud forensics investigators. For example, National Institution for Standards and Technology have started studying challenges faced by cloud forensics investigators.

Even though there is an absence of standard, organizations are still experiencing pressure to have enough, relevant, complete, and admissible evidence available should an incident occur (Elyas *et al.*, 2015; Sachowski, 2016). Cloud consuming organizations are not different. On top of that, consumers are expected to know the level of cloud forensics readiness in their adopted cloud computing services (Makutsoane and Leonard, 2014).

Studying the nature and characteristics of the cloud, researchers in the domain of cloud forensic have coined up number of issues that a cloud forensic investigator may encounter. This research has categorized these issues into those that existed in the main domain of digital forensics but amplified by the cloud and new issues that came into existence with the usage of cloud computing services. Those forensics issues amplified by the use of cloud computing included but not limited to increase in data volume, encryption, and lack of standards. On the other side, the new set of challenges that has been brought into digital forensics investigations by the adoption of public clouds in enterprises include multi-jurisdiction, multi-tenant, dependence on the cloud service provider, and lack of transparency.

Therefore, in search of answers for those issues, cloud forensics solutions have been proposed by a number of researchers over the past years. Some of the researchers simply presented concepts while others provided details on how a solution can be implemented in practice in cloud environments. Among solutions included cloud forensics process models. Different from existing models, this research investigates a cloud forensic process model that provides internal cloud forensic capabilities to consumers to lower issue of dependency on cloud providers for forensic evidence.

1.2 Problem Background

The use of cloud computing has grown at a rapid rate. According to the Information Assurance Advisory Council of United Kingdom (P Sommer, 2013) a range of businesses, of all sizes, are increasingly moving to cloud platforms, often for reasons of cost. Cloud computing market is expected to grow at a compound annual growth rate of 30% and will reach $270 billion in 2020 as reported by Market Research Media (Zawoad, Hasan and Skjellum, 2015). Nonetheless, cloud computing platforms have experienced security issues including criminal exploitation (Vaquero *et al.*, 2011; Ab Rahman and Choo, 2015; Singh and Chatterjee, 2017).

Like any other digital crime, cloud crime stands for any crime that involves cloud computing in the sense that cloud has been used as a subject, object, or tool for offences against digital data or systems. That is, a cloud can be a subject of a crime when the criminal act is committed within the cloud environment, and a cloud can be an object of a crime when the target of the crime is the data centers and other sections of the cloud that provisions the cloud services to the cloud consumer. Similarly, a cloud can be considered as a tool when the availability of the massive computation power and storage facility of a cloud is used as a means of conducting crimes (Cruz, 2012).

It has already been reported in number of cases that cloud computing has been used for malicious purposes (Goodin, 2011; Magazine, 2014; Zawoad*,* *et al.*, 2015). For example, in 2013, a Chinese gang has exploited cloud file storage services (Dropbox) to distribute its malware in preparation for an initial stage of Distributed Denial of Service (DDoS) attack (Alqahtany *et al.*, 2015).

Since for any action there is a reaction, any security incident that occurs in cloud environments should usually be responded initially in order to verify the type of the incident and the scope of its damage. Subsequently, based on the scope of the damage of the incident, an incident response that may either involve eradication and containment or escalations for further investigations, is invoked (Ab Rahman and Choo, 2015).

Although responding to an incident targeting conventional systems has never been easy, the use of cloud has exacerbated and made it even worse by creating a new venue for digital forensic investigations with different issues and challenges. This new venue has later been introduced as Cloud Forensics (Group; Ruan *et al.*, 2011; Simou *et al.*, 2015).

In this light, similar to digital forensics (Carrier and Spafford, 2004), cloud forensics can also be used for different purposes including due diligence or regularity compliance, troubleshooting, investigation, data and system recovery, and/or log monitoring. Therefore, digital forensic practitioners, both from industry and academia, have then tried to adopt and extend existing digital forensic tools and processes into the cloud environments (Dardick *et al.*, 2011; Quick and Choo, 2014c; Almulla *et al.*, 2014; Ab Rahman and Choo, 2015).

However, lack of physical access to locate devices and digital evidence in a cloud environment caused by the impossible identification of location of the data stored in clouds, and the multi-tenancy nature of the cloud that makes infeasible to seize servers from a data center without violation of the privacy of other tenants, have invalidated the assumption of adopting conventional digital forensic tools and processes in cloud environments.

Consequently, a dependency on the cloud service provider for forensic data collection has become an essential part of investigations pertaining to cloud environments (Alqahtany, *et al.*, 2015; Pichan *et al.*, 2015). Nonetheless, the trustworthiness of the evidential data collected by the cloud provider would also be questionable (Zawoad, Hasan and Grimes, 2015; Zawoad, Hasan and Skjellum, 2015).

In other words, there would be a possibility that the person in charge for the collection of the digital evidence at the cloud provider may not be competent enough to collect evidence in a forensically sound manner. In addition, the evidence may intentionally be destroyed by either colluding with the perpetrator or for reason of not to damage the reputation of the cloud provider.

It can be concluded that cloud forensics issues have become more problematic and solutions that could provide cloud forensics must be sought urgently (Poisel and Tjoa, 2012; Alqahtany*, et al.*, 2015; Pichan *et al.*, 2015; Alex and Kishore, 2017; Simou *et al.*, 2017).

Over the past years, researches on cloud forensic have been heavily active in the domain of digital forensics where several works, that are orthogonal to the contribution of this research, have been introduced as solutions to the challenges in the cloud forensics.

Some research works had their focus only on *cloud forensic readiness* (De Marco, Abdalla*, et al.*, 2014; De Marco, Ferrucci*, et al.*, 2014; Ferguson-Boucher and Endicott-Popovsky, 2012; Makutsoane and Leonard, 2014; Sibiya *et al.*, 2013; Trenwith and Venter, 2013). Researchers did not include in their works, measures a cloud consumer should take once their data residing in the cloud is compromised. Instead, researchers only focus on the preparedness that an organization should achieve prior to adopting a cloud service.

Number of *cloud forensic process models* have been reported in the literature (Cho *et al.*, 2012; Chung *et al.*, 2012; Gebhardt and Reiser, 2013; Guo *et al.*, 2012; Martini and Choo, 2012, 2013, 2014a, 2014b; Povar and Geethakumari, 2014; Quick *et al.*, 2013; Simou*, et al.*, 2015; Spyridopoulos and Katos, 2012; Zawoad*, et al.*, 2015). However, researchers who have proposed cloud forensic process models in the literature did not firstly take into account importance of cloud forensics readiness. In this study, the research argues that cloud forensics readiness is mandatory in the process of collecting and analyzing digital evidence residing in cloud environments. Secondly, one of the weaknesses pertaining to existing cloud forensic process models include a general lack of focus of cloud consumer aspects of cloud forensics. In addition, models did not clearly state importance of live forensic in cloud forensics. As a result, there is a complete lack of dedicated live forensic to remotely investigate cloud data centers.

Some have even gone further by concentrating on specific steps of the process of cloud forensic investigation including *evidence collection and acquisition* (Dykstra and Sherman, 2012; Federici, 2014; Oestreicher, 2014), *evidence examination and analysis* (Anwar and Anwar, 2011; Hale, 2013; Marturana *et al.*, 2012; Quick and Choo, 2013a, 2013b, 2014a), and finally some researchers have proposed *cloud-based technical and conceptual solutions* to counter the cloud forensic challenges (Alex and Kishore, 2017; Alqahtany *et al.*, 2015; Battistoni *et al.*, 2016; Delport *et al.*, 2011; Dykstra and Sherman, 2013; Manoj and Bhaskari, 2016; Marty, 2011; Patrascu and Patriciu, 2015; Roussev *et al.*, 2016; Yan, 2011; Zawoad *et al.*, 2013; Zawoad *et al.*, 2015). Problem with these research works is that researchers only focus on one or two processes, while leaving behind some other processes that cannot be ignored both in conventional and cloud forensics investigations. For instance, some of the missing processes may include evidence preservation and chain of custody. Researcher similarly do not discuss live and readiness processes.

Apart from these solutions there is and have been a lack of a single cloud forensic process model that takes together cloud forensic investigation procedures to support cloud consumers' forensic capability based on cloud environment investigation theories.

1.3 Problem Statement

Due to the infancy of the cloud, digital forensics processes and procedures still lack standards that can be directly applied when digital investigation needs to be carried out in cloud environments (Sibiya, *et al.*, 2013). Lack of accessibility to the data centers, from which clouds are abstracted, is another challenge to cloud consuming organization to conduct forensic investigation to their data stored in cloud. This has created a dependency on the cloud service provider for the collection of potential digital evidence (Pichan, *et al.*, 2015). Even though, a number of researchers have proposed cloud forensic process models in an attempt to capture a process that would have guided investigations pertaining to cloud environments, most of them provided solutions focusing specific processes of cloud forensic investigations. Similarly, some of the researchers focused on provider oriented methodologies while others only focused on the law enforcement aspect. However, these solutions do not facilitate consumer side cloud forensics investigations.

A consumer oriented cloud forensic process model is yet to be developed. It is therefore strongly believe that there must be a process model that would help consumers conduct independent forensic investigations, without or little help of the provider. Having said that, the next section discusses main research questions answered by this research.

1.4 Research Questions

As the overall goal of this research is to develop a cloud forensics process model with cloud consumers in mind, the research questions that have been formulated to be answered by this research are as follows:

i. How can a consumer oriented cloud forensics process model be developed by integrating existing digital and cloud forensic best practices?

ii. How can the developed cloud forensic process model be used by a cloud consumer organization to investigate security incidents happening in cloud computing environments?

iii. How can a bilaterally trusted cloud forensic-as-a-services model be instantiated from the developed cloud forensic process model?

1.5 Research Objectives

The main objective if this research was to tackle current problems of cloud forensics in connection to cloud consumers, by the development of a highly overriding process model. The objectives for this research that would have contributed to the current state of cloud forensics are:

i. To develop a cloud forensic process model by integrating existing best practice models in order to help cloud consuming organizations investigate security incidents in cloud environments.

ii. To validate the utility of the developed cloud forensics process model through a simulated cloud computing environment.

iii. To propose a Cloud Forensics-as-a-service model that can be trusted both by the consumers and providers.

1.6 Scope of the Research

This research would enable cloud consuming organizations to take the initiative of preparing themselves for investigating their adopted cloud services by focusing on infrastructural, operational and legal aspects of readiness. A cloud environment that involved only two actors including cloud consumer and cloud provider has been considered in the research. In other words, it involves a cloud consumer organization that has signed contractual agreements with one cloud service provider that supplied a storage as a service model. Therefore the following aspects are the scope of this research.

i. This research focuses on the business and law enforcement perspectives of cloud forensics.

ii. In the process of model development a total of twenty three digital forensics process models that existed in the literature from 2001 to 2013 have first been reviewed. Subsequently, to select the most appropriate among those twenty three process models, eleven have been selected by mapping them to an inclusion criteria established based on a set of requirements needed for the target process model.

iii. A set of thirteen cloud forensic process models existed from 2012 to 2016, were prepared in order for them to be used in the validation of the proposed process model.

iv. The model has been demonstrated in a simulated private storage as a service cloud environment.

v. Throughout the research Anti-Forensic and Decryption issues, that existed in the bigger domain of digital forensics but exacerbated by the cloud, were not separately considered.

1.7 Significance of the Research

In this digital age, most business are moving to cloud. This has created opening for potentially harmful unanticipated information security incidents (both criminal and civil nature) with the potential to cause considerable direct and indirect damage to organizations. Electronic evidence is fundamental to the successful handling of such incidents. Often, in cloud when evidence is needed to prove fraudulent transactions, trustworthy evidence is not available. Unfortunately, lack of standards or particularly missing procedural aspect make cloud forensic preparedness appear difficult for consuming organizations. This has created a dependency on cloud providers for evidence collection which by itself its trustworthiness is questionable.

Hence, the main importance of this research is that it investigates and tries to get a solution for this explicated problem by developing a cloud forensics process model together with a model that would produce a trusted digital evidence at the premises of the consumer.

1.8 Organization of the Thesis

This thesis consists of eight chapters. The chapters are organized according to different works that involves in this research. The detailed organization of this is described in the following paragraphs.

Chapter 1 describes the general outline of the research by giving a brief introduction and problem of the research. The Objectives and aims of the study have been discussed here. The scope and importance of the research have also been pointed out in this chapter.

Chapter 2 reviews of existing related works and its current status has been studied. It includes review of existing cloud and conventional digital forensic process models used to contribute to the development of the CFPM model. Similarly, the tools used by previous researchers to represent existing process models have also been studied and compared to identify the most appropriate modeling tools that should be used for the representation of CFPM model.

Chapter 3 talks and details the research methodology. The thesis has justified the research method that would successfully lead achievement of the aims of the research. Five phases upon which this research has been carried out are broadly discussed. Finally the big picture of the design of this research has been presented in this chapter.

Chapter 4 presents the development of the first version of the CFPM model. The development process employed in the process of developing the model has been clearly stated in this chapter. Here, a group of process models that could contribute to the development of the model have been selected from the list of the process models reviewed in Chapter 2. A comparison of the developed process model to existing cloud forensic process models to validate its generality is conducted.

Chapter 5 demonstrates the utility of the CFPM model via employing two scenarios. The first scenario prepares a cloud consuming organization for cloud forensics while the second is an investigative scenario that investigates the adequacy of the CFPM model to lead an investigation that involves a cloud storage service. Subsequently, an expert evaluation that has been subjected to the model together with its demonstration has also been discussed in this chapter.

Chapter 6 also demonstrates a bilateral cloud as a service model that is built on the live forensic component of the CFPM model. It discusses a unilaterally collected evidence and a conflict resolution protocol that can be employed if the consumer and provider failed to agree upon the completeness of the evidence.

Chapter 7 concludes the research by discussing the achievements made throughout the path of this research. It also highlights recommendations and future works and the possibility of extending this research.

REFERENCES

Ab Rahman, N. and Choo, K. (2015). Integrating digital forensic practices in cloud incident handling: A conceptual cloud incident handling model. *Cloud Security EcosystemR,* 383-400.

Ab Rahman, N. H., Cahyani, N. D. W. and Choo, K. K. R. (2016). Cloud incident handling and forensic-by-design: cloud storage as a case study. *Concurrency and Computation: Practice and Experience,* p.e3868.

Ab Rahman, N. H. and Choo, K.-K. R. (2015). A survey of information security incident handling in the cloud. *Computers & Security*, 49, 45-69.

Ab Rahman, N. H., Glisson, W. B., Yang, Y. and Choo, K.-K. R. (2016). Forensic-by-design framework for cyber-physical cloud systems. *IEEE Cloud Computing*, 3(1), 50-59.

Adams, R. (2012). *The Advanced Data Acquisition Model (ADAM) &58; A process model for digital forensic practice. Journal of Digital Forensics*, *8*(4), pp.25-48.

Adolph, M., Sutherland, E. and Levin, A. (2009). Distributed computing: Utilities, grids & clouds. *International Telecommunication Union-Technology Watch Report*, 9.

Agarwal, A., Gupta, M., Gupta, S. and Gupta, S. (2011). Systematic digital forensic investigation model. *International Journal of Computer Science and Security (IJCSS)*, 5(1), 118-131.

Al Fahdi, M., Clarke, N. L. and Furnell, S. M. (2013). Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions. Proceedings of the 2013 *Information Security for South Africa, 2013*, 1-8.

Alex, M. E. and Kishore, R. (2017). Forensics framework for cloud computing. *Computers & Electrical Engineering* ,60, pp.193-205.

Alhamad, M., Dillon, T. and Chang, E. (2010). Sla-based trust model for cloud computing. Proceedings of the 2010 *Network-Based Information Systems (NBiS), 2010 13th International Conference on*, 321-324.

Alhamad, M., Dillon, T. and Chang, E. (2011). A survey on sla and performance measurement in cloud computing *On the Move to Meaningful Internet Systems: OTM 2011* (pp. 469-477): Springer.

Alismail, S., Zhang, H. and Chatterjee, S. (2017). A Framework for Identifying Design Science Research Objectives for Building and Evaluating IT Artifacts. Proceedings of the 2017 *International Conference on Design Science Research in Information Systems*, 218-230.

Alliance, C. (2013). The notorious nine: Cloud computing top threats in 2013. *Acessado em*, 12(04).

Almulla, S., Iraqi, Y. and Jones, A. (2014). A state-of-the-art review of cloud forensics. *Journal of Digital Forensics, Security and Law*, 9(4), 2.

Alqahtany, S., Clarke, N., Furnell, S. and Reich, C. (2015). A forensic acquisition and analysis system for IaaS. *Cluster Computing*, 1-15.

Anwar, F. and Anwar, Z. (2011). Digital forensics for eucalyptus. Proceedings of the 2011 *Frontiers of Information Technology (FIT), 2011*, 110-116.

Archer, J. and Boehm, A. (2009). Security guidance for critical areas of focus in cloud computing. *Cloud Security Alliance*, 2, 1-76.

Armstrong, C. and Armstrong, H. (2010). Modeling forensic evidence systems using design science. Proceedings of the 2010 *IFIP Working Conference on Human Benefit through the Diffusion of Information Systems Design Science Research*, 282-300.

Ayad, S. (2013). *Business Process Models Quality: evaluation and Improvement.* (Doctoral dissertation, Paris, CNAM).

Ballou, S. (2010). *Electronic crime scene investigation: a guide for first responders*: Diane Publishing.

Barrett, D. and Kipper, G. (2010). *Virtualization and forensics: a digital forensic investigator's guide to virtual environments*: Syngress.

Barry, D. K. (2012). Web Services, Service-Oriented Architectures, and Cloud Computing: The Savvy Manager's Guide (The Savvy Manager's Guides): Morgan Kaufmann.

Baryamureeba, V. and Tushabe, F. (2004). The enhanced digital investigation process model. Proceedings of the 2004 *Proceedings of the Fourth Digital Forensic Research Workshop*, (pp. 1-9).

Battistoni, R., Di Pietro, R. and Lombardi, F. (2016). CURE—Towards enforcing a reliable timeline for cloud forensics: Model, architecture, and experiments. *Computer Communications*, 91, 29-43.

Becker, J. D. and Bailey, E. IT Controls and Governance in Cloud Computing. In *Proceedings of the Twentieth Americas Conference on Information Systems (AMCIS '14)*(pp. 1-8).

Beebe, N. L. and Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation*, 2(2), 147-167.

Birk, D. and Panico, M. Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing. *Cloud Security Alliance*, 1-31.

Birk, D. and Wegener, C. (2011). Technical issues of forensic investigations in cloud computing environments. Proceedings of the 2011 *Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on*, 1-10.

Biros, D. P., Weiser, M., Burkman, J. and Nichols, J. (2008). Information Sharing: Hackers vs Law Enforcement.

Bogen, A. C. and Dampier, D. A. (2005). Unifying computer forensics modeling approaches: a software engineering perspective. Proceedings of the 2005 *First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05)*, 27-39.

Bradshaw, S., Millard, C. and Walden, I. (2011). Contracts for clouds: comparison and analysis of the terms and conditions of cloud computing services. *International Journal of Law and Information Technology*, 19(3), 187-223.

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J. and Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation computer systems*, 25(6), 599-616.

Cahyani, N. D. W., Martini, B., Choo, K. K. R. and Al-Azhar, A. (2016). Forensic data acquisition from cloud-of-things devices: windows Smartphones as a case study. *Concurrency and Computation: Practice and Experience, 29*(14), p.e3855.

Carrier, B. and Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of digital evidence*, 2(2), 1-20.

Carrier, B. and Spafford, E. H. (2004). An event-based digital forensic investigation framework. Proceedings of the 2004 *Digital forensic research workshop*, 11-13.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*: Academic press.

Checkland, P. and Poulter, J. (2006). *Learning for action: a short definitive account of soft systems methodology and its use, for practitioners, teachers and students*: John Wiley and Sons Ltd.

Cho, C., Chin, S. and Chung, K. S. (2012). Cyber forensic for hadoop based cloud system. *International Journal of Security and its Applications*, 6(3), 83-90.

Chung, H., Park, J., Lee, S. and Kang, C. (2012). Digital forensic investigation of cloud storage services. *Digital investigation*, 9(2), 81-95.

Ciardhuáin, S. Ó. (2004). An extended model of cybercrime investigations. *International Journal of Digital Evidence*, 3(1), 1-22.

Coalition, W. M. (1996). Terminology & glossary. *WFMC Document WFMCTC-1011, Workflow Management Coalition, Avenue Marcel Thiry*, 204, 1200.

Cohen, F. B. (2010). Fundamentals of digital forensic evidence *Handbook of Information and Communication Security* (pp. 789-808): Springer.

Conger, S. (2011). *Process mapping and management*: Business Expert Press, New York CrossRef Google Scholar

Cook, N., Robinson, P. and Shrivastava, S. K. (2006). Design and Implementation of Web Services Middleware to Support Fair Non-repudiable Interactions. *International Journal of Cooperative Information Systems*, 15(04), 565-597.

Cook, N., Shrivastava, S. and Wheater, S. (2002). Distributed object middleware to support dependable information sharing between organisations. Proceedings of the 2002 *Dependable Systems and Networks, 2002. DSN 2002. Proceedings. International Conference on*, 249-258.

Cosic, J., Cosic, Z. and Baca, M. (2011). " Chain of Digital Evidence" Based Model of Digital Forensic Investigation Process. *International Journal of Computer Science and Information Security*, 9(8), 18.

Cruz, X. (2012). The Basics of Cloud Forensics. cloudtimes.org/2012/11/05/the-basics-of-cloudforensics/Nov 2012.

Dardick, N., Baggili, I., Carthy, J. and Kechadi, T. (2011). Survey on cloud forensics and critical criteria for cloud forensic capability: A preliminary analysis. Proceedings of the 2011 *Proceedings of the Conference on Digital Forensics, Security and Law*, 55-70.

Daryabar, F., Dehghantanha, A. and Choo, K.-K. R. (2016). Cloud storage forensics: MEGA as a case study. *Australian Journal of Forensic Sciences*, 1-14.

Datt, S. (2016). *Learning Network Forensics*: Birmingham: Packt Publishing Ltd.

Davenport, T. H. (2013). *Process innovation: reengineering work through information technology*: Harvard Business Press.

De Marco, L., Abdalla, S., Ferrucci, F. and Kechadi, M. T. (2014). Formalization of SLAs for Cloud Forensic Readiness. Proceedings of the 2014 *Proc. ICCSM Conference*, 42-50.

De Marco, L., Ferrucci, F. and Kechadi, T. (2014). Reference Architecture for a Cloud Forensic Readiness System.

De Wit, J. (2013). Continuous Forensic Readiness (Master's thesis, University of Twente).

Delport, W., Köhn, M. and Olivier, M. S. (2011). Isolating a cloud instance for a digital forensic investigation. Proceedings of the 2011 *ISSA*.

Doelitzscher, F. (2014). Security Audit Compliance For Cloud Computing. PhD thesis, Plymouth University, February 2014.

Dresch, A., Lacerda, D. P. and Antunes Jr, J. A. V. (2015). Proposal for the conduct of design science research *Design Science Research* (pp. 117-127): Springer.

Dumas, M., La Rosa, M., Mendling, J. and Reijers, H. A. (2013). *Fundamentals of business process management* (Vol. 1): Springer.

Dykstra, J. (2013). Seizing electronic evidence from cloud computing environments: In *Cloud Technology: Concepts, Methodologies, Tools, and Applications* (pp. 2033-2062). *IGI Global.*

Dykstra, J. and Sherman, A. T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation*, 9, S90-S98.

Dykstra, J. and Sherman, A. T. (2013). Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform. *Digital Investigation*, 10, S87-S95.

Elyas, M., Ahmad, A., Maynard, S. B. and Lonie, A. (2015). Digital forensic readiness: Expert perspectives on a theoretical framework. *Computers & Security*, 52, 70-89.

Endicott-Popovsky, B., Frincke, D. A. and Taylor, C. A. (2007). A theoretical framework for organizational network forensic readiness. *Journal of Computers*, 2(3), 1-11.

Erl, T., Puttini, R. and Mahmood, Z. (2013). *Cloud Computing: Concepts, Technology, & Architecture*: Pearson Education.

Federici, C. (2014). Cloud data imager: A unified answer to remote acquisition of cloud storage areas. *Digital Investigation*, 11(1), 30-42.

Ferguson-Boucher, K. and Endicott-Popovsky, B. (2012). Forensic Readiness in the Cloud (FRC): Integrating Records Management. *Cybercrime and Cloud Forensics: Applications for Investigation Processes: Applications for Investigation Processes*, 105.

Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M. and Inácio, P. R. (2014). Security issues in cloud environments: a survey. *International Journal of Information Security*, 13(2), 113-170.

Forrester, J. and Irwin, B. (2007). A Digital Forensic investigative model for business organisations'. *IFIPSec 2007*.

Freiling, F. C. and Schwittay, B. (2007). A Common Process Model for Incident Response and Computer Forensics. *IMF*, 7, 19-40.

Gebhardt, T. and Reiser, H. P. (2013). Network Forensics for Cloud Computing. Proceedings of the 2013 *Distributed Applications and Interoperable Systems*, 29-42.

Goodin, D. (2011). Amazon cloud hosts nasty banking Trojan. *The Register*. Available: www.theregister.co.uk/2011/07/29/amazon_hosts_spyeye.

Grobler, C. and Louwrens, C. (2007). Digital forensic readiness as a component of information security best practice *New Approaches for Security, Privacy and Trust in Complex Environments* (pp. 13-24): Springer.

Grobler, C., Louwrens, C. and von Solms, S. H. (2010). A multi-component view of digital forensics. Proceedings of the 2010 *Availability, Reliability, and Security, 2010. ARES'10 International Conference on*, 647-652.

Grobler, C. P. (2011). *A Digital Forensic Management Framework.* (Doctoral dissertation, University of Johannesburg).

Grobler, M. (2013). The Need for Digital Evidence Standardisation. *Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security*, 234.

Groesser, S. N. and Schwaninger, M. (2012). Contributions to model validation: hierarchy, process, and cessation. *System Dynamics Review*, 28(2), 157-181.

Group, N. C. C. F. S. W. NIST Cloud Computing Forensic Science Challenges (Draft NISTIR 8006)(2014).

Guo, H., Jin, B. and Huang, D. (2011). Research and review on computer forensics *Forensics in Telecommunications, Information, and Multimedia* (pp. 224-233): Springer.

Guo, H., Jin, B. and Shang, T. (2012). Forensic investigations in cloud environments. Proceedings of the 2012 *Computer Science and Information Processing (CSIP), 2012 International Conference on*, 248-251.

Hale, J. S. (2013). Amazon cloud drive forensic analysis. *Digital Investigation*, 10(3), 259-265.

Hannan, M., Frings, S., Broucek, V. and Turner, P. (2003). *Forensic computing theory and practice: towards developing a methodology for a standardised approach to computer misuse.* (Doctoral dissertation, Edith Cowan University).

Hay, B. and Nance, K. (2008). Forensics examination of volatile system data using virtual introspection. *ACM SIGOPS Operating Systems Review*, 42(3), 74-82.

Henry, P., Williams, J. and Wright, B. (2013). The SANS Survey of Digital Forensics and Incident Response. *A white paper, SANS analyst program.*

Hevner, A. and Chatterjee, S. (2010). *Design science research in information systems.*In *Design research in information systems* (pp.9-22). Springer, Boston, MA..

Hevner, A. R. (2007). A three cycle view of design science research. *Scandinavian journal of information systems*, 19(2), 4.

Hitchcock, B., Le-Khac, N.-A. and Scanlon, M. (2016). Tiered forensic methodology model for Digital Field Triage by non-digital evidence specialists. *Digital investigation*, 16, S75-S85.

Hooper, C., Martini, B. and Choo, K.-K. R. (2013). Cloud computing and its implications for cybercrime investigations in Australia. *Computer Law & Security Review*, 29(2), 152-163.

Horrigan, J. (2008). *Use of cloud computing applications and services*: Pew Internet & American Life Project.

Ieong, R. S. (2006). FORZA–Digital forensics investigation framework that incorporate legal issues. *digital investigation*, 3, 29-36.

Jansen, W. and Grance, T. (2011). Guidelines on security and privacy in public cloud computing. *NIST special publication*, 800, 144.

Jawale, N. (2012). *Locating and extracting digital evidence from hosted virtual desktop infrastructures: cloud context.* (Doctoral dissertation, Auckland University of Technology).

Johannesson, P. and Perjons, E. (2014). *An introduction to design science*: Springer. Springer, Singapore CrossRef Google Scholar

Johansson, L.-O., Wärja, M. and Carlsson, S. (2012). An evaluation of business process model techniques, using Moody's quality criterion for a good diagram. In *CEUR Workshop proceedings* (Vol. 963, pp. 54-64).

Katz, M. and Montelbano, R. (2013). Cloud Forensics. *The Senator Patrick Leahy Center for Digital Investigation, Champlain College*, 4.

Kearney, K. T. and Torelli, F. (2011). The SLA model *Service Level Agreements for Cloud Computing* (pp. 43-67): Springer.

Kent, K., Chevalier, S., Grance, T. and Dang, H. (2006). Guide to integrating forensic techniques into incident response. *NIST Special Publication*, 800-886.

Kleppe, A. G., Warmer, J., Bast, W. and Explained, M. (2003). The model driven architecture: practice and promise: Addison-Wesley Longman Publishing Co., Inc., Boston, MA.

Köhn, M., Eloff, J. H. and Olivier, M. S. (2008). UML Modelling of Digital Forensic Process Models (DFPMs). Proceedings of the 2008 *ISSA*, 1-13.

Köhn, M., Olivier, M. S. and Eloff, J. H. (2006). Framework for a Digital Forensic Investigation. Proceedings of the 2006 *ISSA*, 1-7.

Kohn, M. D., Eloff, M. M. and Eloff, J. H. (2013). Integrated digital forensic process model. *Computers & Security*, 38, 103-115.

Kruse II, W. G. and Heiser, J. G. (2001). *Computer forensics: incident response essentials*: Pearson Education.

Kushner, D. (2013). The real story of stuxnet. *IEEE Spectrum*, 50(3), 48-53. Available: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

Kyei, K., Zavarsky, P., Lindskog, D. and Ruhl, R. (2013). A Review and Comparative Study of Digital Forensic Investigation Models *Digital Forensics and Cyber Crime* (pp. 314-327): Springer.

Lalla, H. and Flowerday, S. (2010). Towards a Standardised Digital Forensic Process: E-mail Forensics. Proceedings of the 2010 *ISSA*,

Lee, S., Savoldi, A., Lim, K. S., Park, J. H. and Lee, S. (2010). A proposal for automating investigations in live forensics. *Computer Standards & Interfaces*, 32(5), 246-255.

Lei, Y. and Cui, Y. (2013). Research on Live Forensics in Cloud Environment. In *2nd International Symposium on Computer, Communication, Control and Automation (3CA).*

Leibolt, G. (2010). The Complex World of Corporate CyberForensics Investigations *CyberForensics* (pp. 7-27): Springer.

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., et al. (2011). NIST cloud computing reference architecture. *NIST special publication*, 500, 292.

Macıas, M., Fitó, J. O. and Guitart, J. (2010). Rule-based SLA management for revenue maximisation in cloud computing markets. Proceedings of the 2010 *Proceedings of the 6th IEEE/IFIP International Conference on Network and Service Management (CNSM)*, 354-357.

Magazine, I. (2014). DDoS-ers launch attacks from Amazon EC2: http://www.infosecuritymagazine.com/news/ddos-ers-launch-attacksfrom-amazon-ec2/, July.

Makutsoane, M. P. and Leonard, A. (2014). A conceptual framework to determine the digital forensic readiness of a Cloud Service Provider. Proceedings of the 2014 *Management of Engineering & Technology (PICMET), 2014 Portland International Conference on*, 3313-3321.

Mangiuc, D. M. (2011). Enterprise 2.0-is the market ready. *Journal of Accounting and Management Information Systems*, 10(4), 516-534.

Manoj, S. K. A. and Bhaskari, D. L. (2016). Cloud Forensics-A Framework for Investigating Cyber Attacks in Cloud Environment. *Procedia Computer Science*, 85, 149-154.

Martini, B. and Choo, K.-K. R. (2012). An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation*, 9(2), 71-80.

Martini, B. and Choo, K.-K. R. (2013). Cloud storage forensics: ownCloud as a case study. *Digital Investigation*, 10(4), 287-299.

Martini, B. and Choo, K.-K. R. (2014a). Distributed filesystem forensics: XtreemFS as a case study. *Digital Investigation*, 11(4), 295-313.

Martini, B. and Choo, K.-K. R. (2014c). Remote programmatic vCloud forensics: a six-step collection process and a proof of concept. Proceedings of the 2014c *Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on*, 935-942.

Marturana, F., Me, G. and Tacconi, S. (2012). A case study on digital forensics in the cloud. Proceedings of the 2012 *Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2012 International Conference on*, 111-116.

Marty, R. (2011). Cloud application logging for forensics. Proceedings of the 2011 *Proceedings of the 2011 ACM Symposium on Applied Computing*, 178-184.

McKemmish, R. (1999). *What is forensic computing?* : Australian Institute of Criminology Canberra.

McKemmish, R. (2008). *When is digital evidence forensically sound?* In *IFIP International Conference on Digital Forensics* (pp. 3-15). Springer, Boston, MA.

Mendling, J., Reijers, H. A. and van der Aalst, W. M. (2010). Seven process modeling guidelines (7PMG). *Information and Software Technology*, 52(2), 127-136.

Mens, T. and Van Gorp, P. (2006). A taxonomy of model transformation. *Electronic Notes in Theoretical Computer Science*, 152, 125-142.

Molina-Jimenez, C., Cook, N. and Shrivastava, S. (2008). On the feasibility of bilaterally agreed accounting of resource consumption. Proceedings of the 2008 *Service-Oriented Computing–ICSOC 2008 Workshops*, 270-283.

Nolan, R., O'sullivan, C., Branson, J. and Waits, C. (2005). First responders guide to computer forensics (No. CMU/SEI-2005-HB-001). CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

Nunamaker Jr, J. F., Chen, M. and Purdin, T. D. (1990). Systems development in information systems research. *Journal of management information systems*, 7(3), 89-106.

Oestreicher, K. (2014). A forensically robust method for acquisition of iCloud data. *Digital Investigation*, 11, S106-S113.

Orton, I., Alva, A. and Endicott-Popovsky, B. (2012). Legal process and requirements for cloud forensic investigations. *In Cybercrime and Cloud Forensics: Applications for Investigation Processes* (pp. 186-229). IGI Global.

Othman, S. H. and Beydoun, G. (2010). Metamodelling approach to support disaster management knowledge sharing.

Ouyang, C., Dumas, M., Van Der Aalst, W. M., Ter Hofstede, A. H. and Mendling, J. (2009). From business process models to process-oriented software systems. *ACM transactions on software engineering and methodology (TOSEM)*, 19(1), 2.

Palmer, G. (2001). A road map for digital forensic research. Proceedings of the 2001 *First Digital Forensic Research Workshop, Utica, New York*, 27-30.

Pandey, P. and De Haes, S. (2015). A Variable Payout Information Security Financial Instrument and Trading Mechanism to Address Information Security Risk. Proceedings of the 2015 *2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, 17-25.

Patrascu, A. and Patriciu, V.-V. (2015). Logging for Cloud Computing Forensic Systems. *International Journal of Computers Communications & Control*, 10(2), 222-229.

Peffers, K., Tuunanen, T., Rothenberger, M. A. and Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, 24(3), 45-77.

Peixoto, D., Batista, V., Atayde, A., Borges, E., Resende, R. and Pádua, C. (2008). A comparison of BPMN and UML 2.0 activity diagrams. In *VII Simposio Brasileiro de Qualidade de Software* (Vol. 56, p. 012010).

Perumal, S. (2009). Digital forensic model based on Malaysian investigation process. *International Journal of Computer Science and Network Security*, 9(8), 38-44.

Pichan, A., Lazarescu, M. and Soh, S. T. (2015). Cloud forensics: Technical challenges, solutions and comparative analysis. *Digital Investigation*, 13, 38-57.

Pilli, E. S., Joshi, R. and Niyogi, R. (2010a). A generic framework for network forensics. *International Journal of Computer Applications*, 1(11).

Pilli, E. S., Joshi, R. C. and Niyogi, R. (2010b). A framework for network forensic analysis. Proceedings of the 2010b *Information and Communication Technologies*, 142-147.

Pilli, E. S., Joshi, R. C. and Niyogi, R. (2010c). Network forensic frameworks: Survey and research challenges. *Digital Investigation*, 7(1), 14-27.

Pipek, V., Wulf, V. and Johri, A. (2012). Bridging artifacts and actors: expertise sharing in organizational ecosystems. *Computer Supported Cooperative Work (CSCW)*, 21(2-3), 261-282.

Poisel, R. and Tjoa, S. (2012). Discussion on the challenges and opportunities of cloud forensics *Multidisciplinary Research and Practice for Information Systems* (pp. 593-608): Springer.

Povar, D. and Geethakumari, G. (2014). A Heuristic Model for Performing Digital Forensics in Cloud Computing Environment *Security in Computing and Communications* (pp. 341-352): Springer.

Prat, N., Comyn-Wattiau, I. and Akoka, J. (2014). Artifact Evaluation in Information Systems Design-Science Research-a Holistic View. Proceedings of the 2014 *PACIS*, 23.

Quick, D. and Choo, K.-K. R. (2013a). Digital droplets: Microsoft SkyDrive forensic data remnants. *Future Generation Computer Systems*, 29(6), 1378-1394.

Quick, D. and Choo, K.-K. R. (2013c). Dropbox analysis: Data remnants on user machines. *Digital Investigation*, 10(1), 3-18.

Quick, D. and Choo, K.-K. R. (2014a). Google Drive: Forensic analysis of data remnants. *Journal of Network and Computer Applications*, 40, 179-193.

Quick, D. and Choo, K.-K. R. (2014d). Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digital Investigation*, 11(4), 273-294.

Quick, D., Martini, B. and Choo, R. (2013). *Cloud storage forensics*: Syngress. Amsterdam, The Netherlands: Elsevier, 2013.

Ranabahu, A. H. and Maximilien, E. M. (2009). A best practice model for cloud middleware systems.

Reilly, D., Wren, C. and Berry, T. (2010). Cloud computing: Forensic challenges for law enforcement. Proceedings of the 2010 *Internet Technology and Secured Transactions (ICITST), 2010 International Conference for*, 1-7.

Reith, M., Carr, C. and Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence*, 1(3), 1-12.

Robinson, P., Cook, N. and Shrivastava, S. (2005). Implementing fair non-repudiable interactions with web services. Proceedings of the 2005 *EDOC Enterprise Computing Conference, 2005 Ninth IEEE International*, 195-206.

Rochwerger, B., Breitgand, D., Levy, E., Galis, A., Nagin, K., Llorente, I. M., et al. (2009). The reservoir model and architecture for open federated cloud computing. *IBM Journal of Research and Development*, 53(4), 4: 1-4: 11.

Rogers, M. K., Goldman, J., Mislan, R., Wedge, T. and Debrota, S. (2006). Computer forensics field triage process model. *Journal of Digital Forensics, Security and Law*, 1(2), 19-38.

Rossi, M., Ramesh, B., Lyytinen, K. and Tolvanen, J.-P. (2004). Managing evolutionary method engineering by method rationale. *Journal of the Association for Information Systems*, *5*(9), p.12.

Roussev, V., Ahmed, I., Barreto, A., McCulley, S. and Shanmughan, V. (2016). Cloud forensics–Tool development studies & future outlook. *Digital Investigation*, 18, 79-95.

Roussev, V., Quates, C. and Martell, R. (2013). Real-time digital forensics and triage. *Digital Investigation*, 10(2), 158-167.

Rowlingson, R. (2004). A ten step process for forensic readiness. *International Journal of Digital Evidence*, 2(3), 1-28.

Ruan, C. and Huebner, E. (2009). Formalizing computer forensics process with UML. Proceedings of the 2009 *International United Information Systems Conference*, 184-189.

Ruan, K. and Carthy, J. (2013a). Cloud Computing Reference Architecture and Its Forensic Implications: A Preliminary Analysis *Digital Forensics and Cyber Crime* (pp. 1-21): Springer.

Ruan, K. and Carthy, J. (2013c). Cloud Forensic Maturity Model *Digital Forensics and Cyber Crime* (pp. 22-41): Springer.

Ruan, K., Carthy, J., Kechadi, T. and Baggili, I. (2013). Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. *Digital Investigation*, 10(1), 34-43.

Ruan, K., Carthy, J., Kechadi, T. and Crosbie, M. (2011). Cloud forensics *Advances in digital forensics VII* (pp. 35-46): Springer.

Ruan, K., James, J., Carthy, J. and Kechadi, T. (2012). Key Terms for Service level agreements to support cloud forensics *Advances in Digital Forensics VIII* (pp. 201-212): Springer.

Selamat, S. R., Yusof, R. and Sahib, S. (2008). Mapping process of digital forensic investigation framework. *International Journal of Computer Science and Network Security*, 8(10), 163-169.

Shariati, M., Dehghantanha, A., Martini, B. and Choo, K. (2015). Ubuntu One investigation: Detecting evidences on client machines. *arXiv preprint arXiv:1807.10448*.

Shin, D. and Akkan, H. (2010). Domain-based virtualized resource management in cloud computing. Proceedings of the 2010 *Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2010 6th International Conference on*, 1-6.

Shipley, T. G., CFE, C. and Reeve, H. R. (2006). Collecting Evidence from a Running Computer. *SEARCH, The National Consortium for Justice and Internationals Standards*, 6.

Sibiya, G., Fogwill, T., Venter, H. S. and Ngobeni, S. (2013). Digital forensic readiness in a cloud environment. Proceedings of the 2013 *AFRICON, 2013*, 1-5.

Sibiya, G., Venter, H. S. and Fogwill, T. (2012). Digital forensic framework for a cloud environment.

Simou, S., Kalloniatis, C. and Gritzalis, S. (2017). Modelling Cloud Forensic-Enabled Services. Proceedings of the 2017 *International Conference on Trust and Privacy in Digital Business*, 147-163.

Simou, S., Kalloniatis, C., Mouratidis, H. and Gritzalis, S. (2015). Towards the Development of a Cloud Forensics Methodology: A Conceptual Model. Proceedings of the 2015 *Advanced Information Systems Engineering Workshops*, 470-481.

Singh, A. and Chatterjee, K. (2017). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, 79, 88-115.

Sommer, P. (2005). Directors and corporate advisors' guide to digital investigations and evidence. Cambridge, UK: Information Assurance Advisory Council.

Sommer, P. (2013). Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organisations, Security Advisors and

Lawyers. Version 3.0 Mar 2012. *Режим доступу:* *http://www. iaac. org. uk/_media/DigitalInvestigations2012. pdf*

Spyridopoulos, T. and Katos, V. (2012). Data Recovery Strategies for Cloud Environments. *Cybercrime and Cloud Forensics: Applications for Investigation Processes: Applications for Investigation Processes*, 251.

Stephenson, P. (2002). End-to-end digital forensics. *Computer Fraud & Security*, 2002(9), 17-19.

Stephenson, P. (2003). A comprehensive approach to digital incident investigation. *Information Security Technical Report*, 8(2), 42-54.

Tan, J. (2001). Forensic readiness. *Technical report Stake Organization*, *Cambridge, MA:@ Stake*, 1-23.

Thethi, N. and Keane, A. (2014). Digital forensics investigations in the cloud. Proceedings of the 2014 *Advance Computing Conference (IACC), 2014 IEEE International*, 1475-1480.

Thorpe, S., Grandison, T., Campbell, A., Williams, J., Burrell, K. and Ray, I. (2013). Towards a Forensic-based Service Oriented Architecture Framework for Auditing of Cloud Logs. Proceedings of the 2013 *Services (SERVICES), 2013 IEEE Ninth World Congress on*, 75-83.

Trenwith, P. M. and Venter, H. S. (2013). Digital forensic readiness in the cloud. Proceedings of the 2013 *Information Security for South Africa, 2013*, 1-5.

Vaishnavi, V. and Kuechler, W. (2004). Design research in information systems. http://desrist.org/design-research-in-information-systems/

Valjarevic, A. and Venter, H. S. (2012). Harmonised digital forensic investigation process model. Proceedings of the 2012 *Information Security for South Africa (ISSA), 2012*, 1-10.

Van Oorschot, P. C. (2003). Revisiting software protection *Information Security* (pp. 1-13): Springer.

Van Staden, F. and Venter, H. S. (2011). Adding digital forensic readiness to electronic communication using a security monitoring tool. Proceedings of the 2011 *Information Security South Africa (ISSA), 2011*, 1-5.

Vaquero, L. M., Rodero-Merino, L. and Morán, D. (2011). Locking the sky: a survey on IaaS cloud security. *Computing*, 91(1), 93-118.

Veber, J. and Smutny, Z. (2015). Standard ISO 27037: 2012 and collection of digital evidence: Experience in the Czech Republic. Proceedings of the 2015 *European Conference on Cyber Warfare and Security*, 294.

Venable, J., Pries-Heje, J. and Baskerville, R. (2012). A comprehensive framework for evaluation in design science research. Proceedings of the 2012 *International Conference on Design Science Research in Information Systems*, 423-438.

Venable, J. R. (2006). The role of theory and theorising in design science research. Proceedings of the 2006 *Proceedings of the 1st International Conference on Design Science in Information Systems and Technology (DESRIST 2006)*, 1-18.

von Solms, S., Louwrens, C., Reekie, C. and Grobler, T. (2006). A control framework for digital forensics *Advances in Digital Forensics II* (pp. 343-355): Springer.

Wang, Z. and Yu, M. (2007). Modeling Computer Forensics Process from Workflow Perspective. *Journal of Communication and Computer*, 4(1), 55-60.

Weske, M. (2012). Business process management architectures *Business Process Management* (pp. 333-371): Springer.

Wieringa, R. (2010). Relevance and problem choice in design science *Global Perspectives on Design Science Research* (pp. 61-76): Springer.

Wilkinson, S. and Haagman, D. (2010). Good practice guide for computer-based electronic evidence. *Association of Chief Police Officers*.

WILLASSEN, S. Y. and Mjølsnes, S. F. (2005). Digital forensics research. *Retrieved December*, 30(2007), 92-097.

Winter, R. (2008). Design science research in Europe. *European Journal of Information Systems*, 17(5), 470-475.

Wu, T., Disso, J. F. P., Jones, K. and Campos, A. (2013). Towards a SCADA forensics architecture. Proceedings of the 2013 *Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research 2013*, 12-21.

Yan, C. (2011). Cybercrime forensic system in cloud computing. Proceedings of the 2011 *Image Analysis and Signal Processing (IASP), 2011 International Conference on*, 612-615.

Yang, C.-T., Shih, W.-C., Huang, C.-L., Jiang, F.-C. and Chu, W. C.-C. (2014). On construction of a distributed data storage system in cloud. *Computing*, 1-26.

Yusoff, Y., Ismail, R. and Hassan, Z. (2011). Common phases of computer forensics investigation models. *International Journal of Computer Science & Information Technology (IJCSIT)*, 3(3), 17-31.

Zawoad, S., Dutta, A. K. and Hasan, R. (2013). SecLaaS: secure logging-as-a-service for cloud forensics. Proceedings of the 2013 *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*, 219-230.

Zawoad, S. and Hasan, R. (2013a). Cloud forensics: a meta-study of challenges, approaches, and open problems. *arXiv preprint arXiv:1302.6312*.

Zawoad, S. and Hasan, R. (2013b). Digital Forensics in the Cloud: ALABAMA UNIV IN BIRMINGHAM.

Zawoad, S., Hasan, R. and Grimes, J. (2015). LINCS: Towards building a trustworthy litigation hold enabled cloud storage system. *Digital Investigation*, 14, S55-S67.

Zawoad, S., Hasan, R. and Skjellum, A. (2015). OCF: An Open Cloud Forensics Model for Reliable Digital Forensics. Proceedings of the 2015 *Cloud Computing (CLOUD), 2015 IEEE 8th International Conference on*, 437-444.